

Appln No. 09/900,224
Amdt date February 3, 2006
Reply to Office action of November 3, 2005

REMARKS/ARGUMENTS

In the Office action dated November 3, 2005, claims 1 - 4, 7 - 9 and 11 - 16 were rejected under 35 U.S.C. § 102 and claims 1 - 16 were rejected under 35 U.S.C. § 112. Claims 5 and 10 were objected to as being dependent upon a rejected base claim, but were deemed allowable if rewritten in independent form including all limitations of the base claim and any intervening claims and to overcome the rejection under 35 U.S.C. § 112.

By this Amendment, Applicant has amended claims 1, 3, 7 - 9 and 13 - 16 and added claims 17 and 18. Reconsideration and reexamination are hereby requested for claims 1 - 18 that are now pending in this application.

Response to the 35 U.S.C. § 112 Rejection of the Claims

The Examiner rejected claims 1 - 16 under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. Specially, the Examiner objected to the use of the term “inversely hash” and other similar terms.

Applicant submits that in view of the teachings of the specification, that the meaning of the term “inversely hash” would be apparent to one skilled in the art and there is, therefore, adequate support in the specification for such a term. For example, the specification discusses at page 6, lines 6 - 22 that a transformation may use a hash function and that “any transformation in conjunction with an appropriate inverse transformation may be used to conceal the source parameter signal.” Applicant submits that it is known that for certain hash functions (typically excluding, however, so-called one-way hash functions) the original parameter may be determined if, for example, the hashed parameter and hash algorithm are known. Nevertheless, to expedite the prosecution of this application, Applicant has amended the claims to replace the phrases such as “inversely hash” with phrases such as “inverse transform.”

Response to the 35 U.S.C. § 102 Rejection of the Claims

Claims 1 - 4, 7 - 9 and 11 - 16 were rejected under 35 U.S.C. § 102(e) as being anticipated by Lotspiech et al, U.S. Patent No. 6,118,873 (hereafter referred to as "Lotspiech"). Claims 1, 7 and 13 are independent. The remaining claims depend on either claim 1, 7 or 13.

Lotspiech is directed to a system for updating keys in a set top box 26 (Figure 1) to prevent cloned set top boxes (i.e., unauthorized set top boxes) from being able to decrypt encrypted broadcasts. To this end, Lotspiech generates a matrix 32 of device keys (Figure 3) and provides a subset of the device keys in the matrix to each set top box. Lotspiech at column 5, lines 15 - 19 and 41 - 45. Lotspiech does not specifically state how the device keys are loaded into the set top boxes. However, it may be inferred that they are loaded into the set top boxes when the set top boxes are manufactured. See Lotspiech at column 5, lines 55 - 59 ("Once the device keys 'S' of the devices 18 have been assigned and the devices 18 placed in use, programs, including digital video programs, can be securely transmitted from the source 16 to the various user video devices 18 using the logic shown in FIG. 4.").

In the event a licensing agency determines that a set top box has been cloned, the licensing agency generates a session key block that it sends it to all of the set top boxes. Generating the session key block involves encrypting several session numbers x_i with the device keys. Lotspiech at Figure 4, blocks 38 and 40 and column 5, line 58 - column 6, line 2. The session key block is then sent to the set top boxes with the encrypted program (encrypted using a session key) as shown in Figure 6. Lotspiech at column 6, lines 6 - 12.

The set top box uses its device keys and the session key block to generate a common key. Specifically, the set top box uses the device keys to decrypt the encrypted session number from the session key block. The set top box then hashes all of the decrypted session numbers to render the common key. The set top box uses the common key to decrypt the encrypted broadcast data received by the set top box. Lotspiech at column 6, lines 31 - 40.

The above illustrates that Lotspiech teaches that the licensing agency computer uses device keys to encrypt session numbers and uses a session key to encrypt the broadcast. Lotspiech also teaches that the set top box uses its device keys to decrypt the encrypted session

numbers and from the session numbers generates the common session key that is used to decrypt the encrypted broadcast.

Applicant notes that the Office action did not state which data in Lotspiech is believed to read on the signals of the claims (e.g., the control signal, the parameter signal, etc.). For the purposes of the discussion that follows Applicant will assume that the Examiner contends that the session number of Lotspiech reads on the claimed control signal.

Claim 1 recites in part: “transmitting by the first device to the second device the control signal and the encrypted or hashed parameter signal and control signal.” Lotspiech does not teach or suggest transmitting both the control signal and, for example, the encrypted portion of the control signal. As discussed above while Lotspiech does send the encrypted session number, it does not also send the session number.

Similarly, Lotspiech does not teach or suggest “receiving by the second device from the first device the control signal and the encrypted or hashed parameter signal and control signal” as claimed in claim 1.

Also, in the absence of a received control signal as claimed, Lotspiech does not teach or suggest “using by the second device the control signal to decrypt or inversely transform the encrypted or hashed parameter signal and control signal” as claimed in claim 1.

Claim 7 recites, in part: “receive a control signal comprising a key index and an encrypted or hashed signal that comprises an encrypted or hashed form of a parameter signal and a portion of the control signal.” As discussed above, Lotspiech never sends or receives both a control signal and, for example, an encrypted portion of the control signal.

Claim 13 recites, in part: “generating, by the first device, a control signal comprising a key index” and “transmitting, by the first device to the second device, the control signal and the encrypted or hashed signal.” The session number of Lotspiech does not comprise a key index. Rather, as explained at column 5, lines 59 - 61 the “session numbers ‘ x_i ’ are randomly generated.” That is, they are random numbers, not indices. While Lotspiech may discuss the matrix in term of indices, such indices are not transmitted from a first device to a second device as claimed.

Appln No. 09/900,224
Amdt date February 3, 2006
Reply to Office action of November 3, 2005

In view of the above, Applicant respectfully submits that claims 1, 7 and 13 are not anticipated by or obvious in view of the cited art. The claims that depend on claim 1, 7 or 13 also are patentable over the cited references for the reasons set forth above. In addition, these dependent claims are patentable over the cited references for the additional limitations that these claims contain.

CONCLUSION

In view of the above remarks Applicant submits that the claims are patentably distinct over the cited references and that all the objections/rejections to the claims have been overcome. Reconsideration and reexamination of the above application is requested.

Respectfully submitted,
CHRISTIE, PARKER & HALE, LLP

By



Stephen D. Burbach
Reg. No. 40,285
626/795-9900

SDB/vsj
SDB PAS656802.1-*02/3/06 5:42 PM